UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/583,406	05/31/2000	Heather Maria Hinton	AUS990922US1	3011

7590 05/07/2004

LAW OFFICE OF JOSEPH R. BURWELL
P.O. BOX 28022
AUSTIN, TX 78755-8022

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	3

DATE MAILED: 05/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/583,406	HINTON ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 May 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *3* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 7-11, 14, 18-19, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges, Jr. et al (US-6510464).

As per **claims 1, 18, and 23**, Grantges, Jr. et al discloses a method for determining whether to allow access to a protected resource from a server (Col 1 lines 11-18), comprising the steps of: at a client, responsive to a request to retrieve the protected resource, generating a piece of data (Col 2 lines 1-5 and Col 10 lines 59-67) which can be used to authenticate that the request is bound to a given identity contained in a cookie previously set by an authentication server (Col 10 lines 59-67); Forwarding the piece of data to the server in the request; at the server, determining whether the piece of data is valid (Col 10 lines 59-67); and if the piece of data is valid, executing an access control decision to determine whether to invoke the request (Col 10 lines 59-67). However, Grantges, Jr. et al do not teach the use of the piece of data one-time only to authenticate specifically. Nevertheless, Grantges, Jr. et al do mention

different embodiments on the authenticate cookie's utility that one of ordinary skill in the art can implicitly recognize the one-time usage (Col 11 lines 1-8). It is obvious at the time of the invention was made for one of ordinary skill in the art to implement the one-time use of the piece of data in order to maximize the authentication security accessing a network. Repetitive use of the authentication data will increase the risk of exposing the sensitive data to hackers. Furthermore, limiting the time usage to the piece of data is well known in the art (Col 11 lines 1-8). For claims 18 and 23, Grantges, Jr. et al do disclose the program code (Col 1 lines 64-67 and Col 2 lines 1-11) to collect information for authentication and process the info.

As per **claims 7, 8, 9, 10, and 14,** Grantges, Jr. et al disclose the method as described in Claims 1 and 11. Grantges, Jr. et al also explicitly teach the cookie includes a userid, the server identity, and a URL pointing to a location at the server that includes a script (Col 10 lines 6-25), and an access control token (Col 10 lines 11-13). The authentication cookie (Col 9 line 55) includes a user digital certificate (userID) and a range of URL's for which the cookie is valid (Col 9 lines 62-65). The URL is also use to identify the server (Server Identity) (Col 10 line 51). The script is located on the proxy server, which is in the same domain or network as the application server or called protected resource (Col 8 lines 15-25), also called authorization plug-in (Col 10 line 59-61); and its job is to validate the authentication cookie. The access control token is referred as an applications list cookie (Col 10 line 15), which includes a list of authorized application for the user to access. It is obvious at the time of the invention was made

for one of ordinary skill in the art to utilize the same system in their invention to carry out an authorization process for the protected resource.

As per **claims 11**, Grantges et al discloses a method of accessing a protected resource at a server, comprising the steps of: at the server, receiving a request for a URL (Col 8 lines 15-28) together with an identity cookie (Col 8 lines 13-30) and an authentication token associated with the request; determining whether the authentication token is valid; if the authentication token is not valid, returning to a requesting client an access denied message; and if the authentication token is valid, executing an access decision function to determine whether to allow access to the protected resource.

As per **claim 19**, Grantges, Jr. et al discloses the computer program product as described in Claim 18 further including a signed applet for installing the code in the client computer (Col 4 lines 33-65).

Claims 16-17, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges, Jr. et al (US-6510464) and Linden et al (US-6360254).

As per **claims 16, 17, and 27**, Grantges, Jr. et al disclose the computer program product as described in Claim 23. Howerver, Grantges Jr. et al do not further including code for saving the timestamp and the authentication token in a data structure to prevent replay of the authentication token. Nevertheless, Linden et al disclose the

"System and method for providing secure URL-Based access to private resources" invention that completely teaches the feature (Col 6 lines 51-55). The token here is generated either of a timestamp, server identification (hardware device pseudo-random sequence of value (Col 5 lines 2-5)), userid, timestamp, or even a random number (Col 4 lines 63-67). It is obvious at the time of the invention was made for one of ordinary skill in the art to incorporate the feature in the claimed invention for security purpose.

Claims 2, 3, 12, 20, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges, Jr. et al (US-6510464) in view of Davis et al (US-6064736) and further in view of Payne et al (US-5715314).

As per **claim 2**, Grantges, Jr. et al disclose the method as described in claim 1. However, Grantges, Jr. et al does not discloses the use piece of data is generated by applying a given function to a URL of the protected resource, a timestamp, a nonce, server identity, and the client's identity.

Nevertheless, Linden et al discloses different method to generate a token (can be interpreted as cookie) by encrypting the timestamp (Col 4 line 64) or by a pseudo-random number generation algorithm (nonce);

Davis et al teach the use of hashing the nonce from the server, and the PW' (password of the user which is the client id) with the server's name (Server ID) to create the secretHash key (Col 6 lines 1-5) for authentication;

And Payne et al teach the use of URL hashing (Col 5 lines 40-45) for authentication.

Therefore, it is obvious at the time of the invention was made for one of ordinary skill in the art to combine Grantges, Jr. et al, Linden et al, Davis et al, and Payne et al's teaching to strengthening the security of the piece of data usage by using the timestamp and a non-repeating random number with the URL, userid, and server id. Further more, the use of a nonce and timestamp together will definitely restrict the piece of data usage to only one time.

As per **claims 3, 12, 20, and 24**, Grantges, Jr. et al, Linden et al, and Davis et al disclose the method as described in Claims 2, 11, and 18. However, Grantges, Jr. et al, Linden et al, and Davis et al do not teach the function get calculated with a given key to become the Message authentication code (MAC) for authentication. Nevertheless, Payne et al do teach the feature. Payne et al disclose the invention "Network sales system" which uses the key to define the hash function of the information in the payment URL to generate the URL authenticator (Col 5 lines 40-45). The URL authenticator is the message authentication code (MAC). Adding the nonce and the timestamp to generate the MAC will definitely prevent the replay of the cookie; The URL can be interpreted as the server identity and the client identity must also necessary in-order to authenticate the server and to distinct the originality of the cookie. Therefore, It is obvious at the time of the invention was made for one of ordinary skill in the art to understand that the combination of the teaching above will increase the security for accessing a protected resource. It is also obvious that a program code or a script in a computer medium is necessary to execute the calculation.

Claim 4, 13, 15, 21, 22, and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable Grantges, Jr. et al (US-6510464) in view of Linden et al (US-6360254), further in view of Davis et al (US-6064736), further in view of Payne et al (US-5715314), and further in view of Juels (US-6446052).

As per **claim 4, 13, 21, 22, and 25**, Grantges, Jr. et al, Linden et al, Davis et al, and Payne et al discloses the method as described in Claim 3, 12, and 21. However, Grantges, Jr. et al, Linden et al, Davis et al, and Payne et al do not teach the method using the symmetric key to binds the piece of data to the user identity. Nevertheless, Juels discloses the method clearly (Col 7 lines 14-26 and Col 8 line 3). The user identity is the IDv, and the piece of data or MAC (Col 8 line 3) is the trustee token Mi or coin (Col 7 lines 41-44). In Col 7 lines 14-26, Juels specifically teach the mapping of a user's identity to the digital coin (piece of data) using the symmetric key encryption. It is obvious at the time of the invention was made to one of ordinary skill in the art to implement the same method of Juels with Linden et al, and Payne et al to distinguish and identify each MAC when authenticate and at the same increase the security to prevent imposter.

As per **claims 15 and 26**, Grantges, Jr. et al, Linden et al, Davis et al, Payne et al and Juels disclose the method as described in Claims 12 and 25 wherein the step of determining whether the authentication token is valid includes the steps of: calculating a

message authentication code; evaluating whether the message authentication code is the same as the MAC in the authentication token. It is obvious at the time of the invention was made for one of ordinary skill in the art to understand that the validation steps of authentication token must be the backward process of the engineering the token in-order to understand the received information. Therefore, it is obviously exist in the system.

Claims 5, and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges, Jr. et al (US-6510464) in view of Linden et al (US-6360254), further in view of Davis et al (US-6064736), further in view of Payne et al (US-5715314), further in view of Juels (US-6446052), and further in view of Gurevich et al (US-2002/0178370).

As per **claim 5**, Grantges, Jr. et al, Linden et al, Davis et al, Payne et al, and Juels discloses the method as described in Claim 4. However, they do not teach the symmetric key that is generated by applying a one-way hash function to a shared client-server key kc, the server identity, and a nonce from the server. Nevertheless, Gurevich et al completely teach this method and the use of it as a symmetric key (Par 0068 in the mid paragraph). The token key and the PIN are used as an encryption key between the server and the client. The SKP is the server side key component generated by a random number engine, at the same is the server key or can be interpreted as server identity (Para 0068). It would be obvious at the time of the invention was made for one of ordinary skill in the art to combine the symmetric key

generation method of Gurevich et together with inventors in claim 4. The incorporation will successfully create a strong and unique key to bind the authentication data securely and then transmit it to the server for authentication (Para 0069).

As per **claim 6**, Grantges, Jr. et al, Linden et al, Davis et al, Payne et al, Jues and Gurevich et al disclose the method as described in Claim 5. The feature of the shared client-server key generated by applying a one-way hash function to a user password is completely anticipated by Davis et al (Col 2 lines 15-25). Davis et al teach the use of hashed password to establish a session between the server and the client to ensure unwanted intruders. It is obvious at the time of the invention was made for one of ordinary skill in the art to recognize that the feature is necessary to incorporate with authentication mechanism to a network for strengthening the security.

Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges, Jr. et al (US-6510464) in view of Davis et al (US-6064736), further in view of Gurevich et al (US-2002/0178370), and further in view of Payne et al (US-5715314).

As per claim 28, Grantges, Jr. et al discloses a method for issuing an access request from a client browser to a server hosting a protected resource (the application database) (Col 4 lines 36-40 and lines 61-65), wherein an identity cookie has been set on the client browser by an authentication server (Proxy server). However, Grantges, Jr. et al do not teach what the method comprises of.

Nevertheless, Payne et al disclose the "Network sales system" invention includes the uses a key shared by the merchant (server) and the operator (client) to generate the payment URL authenticator (Message authentication code). The URL authenticator (MAC) includes a domain identifier (URL and time tracking mechanism to expire the cookie (which must also includes a timestamp) (Col 5 lines 26-46).

Gurevich et al teach the authentication method that includes sending the encrypted data item (Para 0068) (Piece of data), which is also called authentication message (MAC) (Para 0057), with the unencrypted piece of data to the server for validity (Para 0068). The data item composes of the Identification (ID) (user ID) and the server side key (server ID). Gurevich et al also mention the user may arbitrary assign the identification data, which could be a timestamp (Para 0069).

Davis et al teach of hashing the nonce from the server and client, and the password to create a key for decryption (Col 3 lines 65-67).

It is obvious at the time of the invention was made for one of ordinary skill in the art to use the teaching of Payne et al to create the MAC and Gurevich et al's method of sending the MAC with the data items, comprising the timestamp, server ID, user ID, and a nonce, which is taught be Davis et al, to the server with the ID cookie in Grantges Jr. et al teaching for validation (Col 3 lines 43-59). Incorporate all the teaching will obviously create a non-replay cookie (caused by the timestamp and the nonce) and a strong authentication process which creates great obstacle for intruders.

Claims 29-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges, Jr. et al (US-6510464) in view of Davis et al (US-6064736), further in view of Gurevich et al (US-2002/0178370), further in view of Payne et al (US-5715314), and further in view of Juels (US-6446052).

As per **claim 29**, Grantges Jr. et al, Davis et al, Gurevich et al, and Payne et al disclose the method as described in Claim 28. However, they do not teach the generating of the MAC upon each request for the protected. Nevertheless, Juels does teach the method clearly in the "Digital Coin Tracing Using trustee tokens" invention (Juels, Col 8 lines 27-43). Therefore, it is obvious at the time of the invention was made for of ordinary skill in the art to incorporate the method to ensure the authenticity of the message authentication code.

As per **claim 30**, Grantges Jr. et al, Davis et al, Gurevich et al, and Payne et al disclose the method as described in Claim 28. However, Grantges Jr. et al, Davis et al, Gurevich et al, and Payne et al do not teach the method using the symmetric key to binds the MAC to the user identity. Nevertheless, Juels discloses the method clearly (Col 7 lines 14-26 and Col 8 line 3). The user identity is the IDv, and the MAC (Col 8 line 3) is the trustee token Mi or coin (Col 7 lines 41-44). In Col 7 lines 14-26, Juels specifically teach the mapping of a user's identity to the digital coin (MAC) using the symmetric key encryption. It is obvious at the time of the invention was made to one of ordinary skill in the art to implement the same method of Juels with Grantges Jr. et al,

Davis et al, Gurevich et al, and Payne et al to distinguish and identify each MAC when authenticate and at the same increase the security to prevent imposter.

As per **claim 31**, Grantges Jr. et al, Davis et al, Gurevich et al, and Payne et al disclose the method as described in Claim 30. However, they do not teach the symmetric key that is generated by applying a one-way hash function to a shared client-server key kc, the server identity, and a nonce from the server. Nevertheless, Gurevich et al completely teach this method and the use of it as a symmetric key (Par 0068 in the mid paragraph). The token key and the PIN are used as an encryption key between the server and the client. The SKP is the server side key component generated by a random number engine, at the same is the server key or can be interpreted as server identity (Para 0068). It would be obvious at the time of the invention was made for one of ordinary skill in the art to combine the symmetric key generation method of Gurevich et together with inventors in claim 4. The incorporation will successfully create a strong and unique key to bind the authentication data securely and then transmit it to the server for authentication (Para 0069).

As per **claim 32**, Grantges Jr. et al, Davis et al, Gurevich et al, and Payne et al disclose the method as described in Claims 5 and 31. The feature of the shared client-server key generated by applying a one-way hash function to a user password is completely anticipated by Davis et al (Col 2 lines 15-25). Davis et al teach the use of hashed password to establish a session between the server and the client to ensure unwanted

intruders. It is obvious at the time of the invention was made for one of ordinary skill in the art to recognize that the feature is necessary to incorporate with authentication mechanism to a network for strengthening the security.

As per **claims 33 and 34,** Grantges Jr. et al, Davis et al, Gurevich et al, and Payne et al disclose the method as described in Claim 28. Grantges, Jr. et al also explicitly teach the cookie includes a userid, the server identity, and a URL pointing to a location at the server that includes a script (Col 10 lines 6-25), and an access control token (Col 10 lines 11-13). The authentication cookie (Col 9 line 55) includes a user digital certificate (userID) and a range of URL's for which the cookie is valid (Col 9 lines 62-65). The URL is also use to identify the server (Server Identity) (Col 10 line 51). The script is located on the proxy server, which is in the same domain, or network as the application server or called protected resource (Col 8 lines 15-25), also called authorization plug-in (Col 10 line 59-61); and its job is to validate the authentication cookie. The access control token is referred as an applications list cookie (Col 10 line 15), which includes a list of authorized application for the user to access.

As per claim 35, Grantges Jr. et al, Davis et al, Gurevich et al, and Payne et al disclose the method as described in Claim 34 wherein the script includes code for identifying whether a MAC is valid (Juels, Col 7 lines 35-45).

Conclusion

Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (703)-305-8914.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (703)-305-4393. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (703)-305-9600.

Linh LD Son

Patent Examiner

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100